

ROPES & GRAY
ONE FRANKLIN SQUARE
1301 K STREET, N.W.
SUITE 800 EAST
WASHINGTON, DC 20005-3333
(202) 626-3900
FAX: (202) 626-3961

ONE INTERNATIONAL PLACE
BOSTON, MA 02110-2624
(617) 951-7000
FAX: (617) 951-7050

30 KENNEDY PLAZA
PROVIDENCE, RI 02903-2328
(401) 455-4400
FAX: (401) 455-4401

CHILDREN'S INTERNET PROTECTION: MORE QUESTIONS THAN ANSWERS

President Clinton signed into law the Children's Internet Protection Act and the Neighborhood Children's Internet Protection Act on December 21, 2000. These acts, attached to the omnibus appropriations law during the last days of the 106th Congress, will require schools and libraries that receive funding under either title III of the Elementary and Secondary Education Act or the Museum and Library Services Act, or that receive universal service discounts for Internet access ("E-rate"), to adopt an Internet safety policy incorporating the use of filtering or blocking technology on computers with Internet access.

Background. Title XVII of the Omnibus Consolidated and Emergency Supplemental Appropriations Act for Fiscal Year 2001 addresses "Children's Internet Protection" in two separate and related provisions. Sections 1701 through 1721 constitute the "Children's Internet Protection Act" (CIPA), requiring certification by covered schools and libraries that an Internet safety policy has been adopted and implemented (which includes use of a "technology protection measure" that blocks or filters certain visual depictions). Sections 1731 through 1733 constitute the "Neighborhood Children's Internet Protection Act," requiring E-rate recipients to adopt and implement an Internet safety policy that goes beyond the protections required in CIPA. The Neighborhood Act requires that the Internet safety policy address such matters as hacking and security of minors using chat rooms and also that there be local notice and a public hearing or meeting to address the proposed policy.

Conundrums, ambiguities, and unanswered questions. Cobbled together from three legislative proposals as a rider to an appropriations act, without benefit of public hearings or committee deliberation on two of the three, the new law unsurprisingly presents a myriad of challenges to those libraries and schools covered by its requirements. Some of the principal challenges lie in understanding the law itself. The discussion below highlights some of the conundrums, ambiguities, and unanswered questions presented by the text of the statute. Some may be answered or clarified by regulations or guidelines from the responsible agencies; for now, they bear serious attention.

1. The "fundamental premise" conundrum: There should be no surprise that the new statute presents problems for affected schools and libraries, for it is based on a fundamentally flawed premise. The law requires covered entities to put in place a "policy of Internet safety that includes the operation of a technology protection measure" Such technology protection measure (TPM) is defined as "specific technology that blocks or filters Internet access to visual

depictions that are—(A) obscene . . . (B) child pornography . . . or (C) harmful to minors.” Hence, the act requires the TPM be technology that actually works!

Alas, not two months earlier the Commission on Child Online Protection (COPA) concluded that it could not say for certain that there is any particular technology that meets the definition of constituting “reasonable measures” to restrict access by minors to harmful materials. Hence, the COPA Commission has effectively said that CIPA may be requiring the impossible. Additionally, no technology that is designed to restrict access by minors to certain Internet materials can avoid blocking access to other material protected by the First Amendment. Nonetheless, a responsible reading of the statute and the intent of Congress would require that the TPM utilized by a school or library be designed and intended to protect children through blocking or filtering Internet access, not that it work. It should be the former, not the latter, to which any certification is addressed.

2. The “dirty picture” limitation. The new law requires that the TPM block or filter Internet access only with regard to “visual depictions.” There is no requirement that technology address narrative material that may be obscene or child pornography or harmful to minors (all defined terms). On the other hand, the Internet safety policy must be much broader and address “access by minors to inappropriate matter” or to “materials harmful to minors.” For the most part, “acceptable use” policies adopted by libraries and schools should be adequate to address these latter issues, recognizing that what is “inappropriate for minors” shall be determined by a local authority.

3. “Tracking” versus “monitoring.” A specific disclaimer in CIPA states that nothing in this title “shall be construed to require the tracking of Internet use by any identifiable minor or adult user.” Yet the certification required must specify that the school or library “is enforcing the operation of such technology protection measure during any use of such computers,” and the required “Internet safety policy” must address safety and security of minors when using e-mail and chat rooms, hacking and other unlawful activities, unauthorized disclosure of a minor’s personal identification information, and restriction of access to materials harmful to minors. Clearly Congress appears to expect some proactive effort on the part of schools and libraries to monitor computer usage by minors, but forbids “tracking” as part of that effort.

4. Consortia confusion and two-tier grant recipients. The new law appears not to contemplate fully that grants from the Department of Education (D. Ed.) and the Institute of Museum and Library Services (IMLS) do not always flow directly from the federal government to the library or school. In most cases the states or a state entity passes through the funds; in others, the ultimate recipients are part of a consortium of institutions where the consortium is the immediate grantee. The timing of implementation and the nature of the certification are confounded by these phenomena.

5. The disabling dilemma. The statute specifically allows disabling of the TPM, but E-rate libraries and schools are not treated the same as those that are covered as ESEA and IMLS grantees. For the former, the TPM may be disabled to allow only adult access; for the latter, an authorized person may disable the TPM for adult or minor use. In both cases, however, the

disabling may occur only “to enable access for bona fide research or other lawful purposes.” Since the viewing of obscene material – even by a minor – may not be *unlawful in some states*, it might be argued that a TPM can be disabled for the asking, even though this was not likely what Congress had in mind.

6. The enforcement enigma. CIPA sets up an enforcement scheme under which the responsible federal agency may withhold federal program payments or suspend E-rate discounts or payments if the recipient “is failing to comply substantially with the requirements of” the law. The D.Ed. and IMLS may also seek a cease and desist order against or enter into compliance agreements with a recipient. A few issues are raised by these provisions.

First, the question of judging “substantial” compliance in an area where full compliance is probably technologically impossible (see item 1 above) can be tricky. Good faith efforts should be the key, but that will depend on agency compliance attitude.

Second, the compliance provision for IMLS is grafted from that applicable to the D.Ed., and it is imperfect. While the IMLS is not generally subject to the General Education Provisions Act remedies, this law may be read as giving IMLS the opportunity to incorporate these measures into its current enforcement procedures.

Third, while the certification requirement is tied to use of federal funds for purchase of computers used to access the Internet or pay for direct costs associated for accessing the Internet, it appears that *all* federal funding under the applicable statute (ESEA, MLSA) must be cut off if certification is not made for the second program year. This contrasts with the approach used for E-rate beneficiaries: the prohibition on receipt of discounted rates without the required certification applies only for Internet access, Internet services, or internal connections.

Finally, because of the targeted nature of the legislation – funds used for computers and Internet connection – libraries and schools remain free to use federal program funds for other purposes and redirect nonfederal funds for computer and Internet use, thus avoiding the reach of the new law. Whether the federal agencies will require some form of negative certification or otherwise will attempt to audit use of funds to ensure that none is used for computer and Internet purposes by noncomplying entities is unknown.

Tomas M. Susman
Ropes & Gray
202-626-3920
tsusman@ropesgray.com

January 13, 2001